AGM列を用いた楕円曲線の有理点位数計算法の超楕円を越える曲線への一般化について (Computer Algebra : Design of Algorithms, Implementations and Applications)

AUTHOR(S):

綾野, 孝則

数理解析研究所講究録
第1666巻 2009年 117-126

AGM列を用いた楕円曲線の有理点位数計算法の超楕円を越える曲線への一般化について

綾野 孝則
TAKANORI AYANO
大阪大学 理学研究科
GRADUATE SCHOOL OF SCIENCE, OSAKA UNIVERSITY *

1 Introduction

G を有限巡回群、α を G の生成元とするとき、$\beta \in G$ に対して、$\beta = \alpha^k$ となる k を求める問題を離散対数問題という。離散対数問題が計算量的に困難であるとき、G を暗号に利用することができる。G として、有限体上の楕円曲線の一つの有理点で生成される群としたものを楕円曲線暗号といい、実用化されている。しかし楕円曲線の群位数が大きい素因数を含まないときは安全でないことが知られている。つまり楕円曲線の群位数を知ることは、楕円曲線暗号の安全性を保障する上で非常に重要である。楕円曲線の定義体を $\mathbf{F}_q, q = p^N$ (p:素数) とするとき、暗号には $p = 2$ で N が大きいときがよい。この条件の下で、楕円曲線の群位数を計算するための現在知られている最も効率のよい方法はAGM列 (算術幾何平均) を用いたMestreの方法である。しかし現在、ある条件の下で、楕円曲線暗号の解読法が見つかっているため、今後の安全性を考えると様々な代数曲線を暗号に利用できるようにすることは重要である。一般の代数曲線の場合は、そのJacobi多様体の有理点全体のなす群を暗号に用いることになる。この場合も安全性を確かめるために、その群位数を計算する必要がある。ここでは、まず楕円曲線におけるMestreの方法について述べた後、Mestreの方法が楕円曲線よりも一般的な代数曲線に拡張できるかという問題について述べる。

2 準備

2.1 楕円曲線

K を体、$\overline{K}$ を K の代数閉包とする。$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$ とする。$a_i \in K$
$E/K := \{(x,y) \in \overline{K}^2 | f(x,y) = 0\} \cup \{O\}$
$\forall (x,y) \in E \backslash \{O\}$ において、$\frac{\partial f(x,y)}{\partial x}, \frac{\partial f(x,y)}{\partial y}$ が共に0になることはないとする。(非特異)
$E(K) := \{(x,y) \in K^2 | f(x,y) = 0\} \cup \{O\}$
E/K を K 上の楕円曲線、$E(K)$ を E の K 有理点という。O を無限遠点という。
以下、$E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ と書く。
ある演算により E は O を単位元とする群になる。$E(K)$ は E の有限部分群になる。
整域 $K[x,y]/ < f(x,y) >$ の商体を $K(E)$ と書き、E/K の関数体という。
$\overline{K}[x,y]/ < f(x,y) >$ の商体を $\overline{K}(E)$ と書く。

*t-ayano@cr.math.sci.osaka-u.ac.jp

2.2 isogeny

$E/K, E'/K$ を K 上の楕円曲線、O, O' をそれぞれ、E, E' の無限遠点とする。
$\phi : E \to E' \quad (x,y) \to (f(x,y), g(x,y)) \quad f,g \in \overline{K}(E) \quad \phi(O) = O$
ϕ を E から E' への isogeny という。$f,g \in K(E)$ のとき ϕ を K 上の isogeny という。
E から E' への isogeny 全体を $Hom(E,E')$ とする。
K 上の isogeny ϕ により、関数体の間の引き戻し写像 $\phi* : K(E') \to K(E) \quad h \to h \circ \phi$ が自然に定義される。
体の拡大 $K(E)/\phi * K(E')$ の拡大次数を ϕ の次数といい、$\deg\phi$ で表す。
$\deg\phi = 1$ のとき、E と E' は K 上同型、$E \cong E'$ であるという。
m を自然数とする。$[m] : E \to E \quad P \to m \cdot P := P + \cdots + P$ とする。
$[m]$ は isogeny になる。
$\phi \in Hom(E,E')$ に対して、$\hat{\phi} \circ \phi = \phi \circ \hat{\phi} = [\deg\phi]$ となる $\hat{\phi} \in Hom(E',E)$ が一意的に存在する。$\hat{\phi}$ を ϕ の dual isogeny という。

2.3 trace

p を K の標数とする。
$E[m] := \{P \in E \mid m \cdot P = O\}$ とする。
素数 $l \neq p$, n:自然数 に対して、$[l] : E[l^{n+1}] \to E[l^n] \quad P \to l \cdot P$ を考える。
$\{E[l^n], [l]\}_{n \geq 1}$ は射影系をなす。
$T_l(E) := \lim_{\leftarrow n} E[l^n]$（逆極限）を E の l 進 Tate 加群という。
$T_l(E)$ は rank 2 の自由 $\mathbf{Z}_l$ (l 進整数) 加群になる。
$End(E) := Hom(E,E)$ とする。
自然な単射準同型 $End(E) \to End_{\mathbf{Z}_l}(T_l(E)) \quad \phi \to \phi_l$ が定義される。
$Tr(\phi) := Tr(\phi_l)$ で定義し、ϕ の trace という。(l のとり方によらない) $Tr(\phi) \in \mathbf{Z}$ となる。

2.4 p 進体

p を素数、$q = p^N$ (N:自然数) とする。
$\mathbf{Q}_p$ を p 進体、$\mathbf{Q}_q$ を $\mathbf{Q}_p$ の N 次不分岐拡大、$\mathbf{Z}_q$ を $\mathbf{Q}_q$ の付値環とする。
$\mathbf{Q}_q$ の剰余体は、$\mathbf{Z}_q/2\mathbf{Z}_q \cong \mathbf{F}_q$ (位数 q の有限体)
$\pi : \mathbf{Z}_q \to \mathbf{F}_q$ を自然な全射準同型 (reduction) とする。

3 楕円曲線の位数計算

$\mathbf{F}_q$ を位数 q の有限体, $q = 2^N$ とする。
$\mathbf{F}_q$ 上の楕円曲線 $\bar{E}/\mathbf{F}_q$ において、$\mathbf{F}_q$ 有理点の個数 $\sharp\bar{E}(\mathbf{F}_q)$ を効率よく計算したい。

Theorem 3.1 (Hasse-Weil)
(1) $\sharp\bar{E}(\mathbf{F}_q) = 1 + q - Tr(Fr_q)$
ここで、$Fr_q : E \to E \quad (x,y) \to (x^q, y^q)$ であり、E の q 乗 Frobenius 写像という。
(2) $|Tr(Fr_q)| \leq 2\sqrt{q}$

$Tr(Fr_q)$ を求めることを考える。

3.1 扱う楕円曲線の限定

任意の楕円曲線は次の形の楕円曲線と $\mathbf{F}_q$ 上同型となる。(つまり、$\mathbf{F}_q$ 有理点の個数は等しい)
$\bar{E}/\mathbf{F}_q : y^2 + xy = x^3 + a_2x^2 + a_6$
簡単な考察から、$a_2 = 0$ のときを考えればよい。([3] section 3.10)
また $j(\bar{E}) \in \mathbf{F}_4$ のとき、$\sharp\bar{E}(\mathbf{F}_q)$ は容易に求まる。([3] Theorem 3.66)
($j(\bar{E})$ は $\bar{E}$ の定義方程式の係数から計算される量で、j-invariant という。([2] p.46))
よって、$j(\bar{E}) \notin \mathbf{F}_4$ としてよい。
以上より扱う楕円曲線は以下のもののみでよい。($\mathbf{F}_q$ の全ての元は平方元であることに注意)

$$\bar{E}/\mathbf{F}_q : y^2 + xy = x^3 - \bar{\alpha}^2 \qquad \bar{\alpha} \notin \mathbf{F}_4 \tag{1}$$

3.2 AGM 列

Proposition 3.2.1 ([1] p.12)
$a, b \in \mathbf{Z}_q$ が次の $1 \sim 3$ を満たすとする。
(1) $a^2 \neq b^2, ab \neq 0$
(2) $a, b \equiv 1 \bmod 4$
(3) $a + b \equiv 2 \bmod 8$
このとき、ab の平方根で $1 \bmod 4$ となるものが一意的に存在する。
それを $\sqrt{ab}$ とすると、$\frac{a+b}{2}, \sqrt{ab}$ は再び $1 \sim 3$ を満たす。

$\alpha \in \mathbf{Z}_q$ を $\bar{\alpha} \in \mathbf{F}_q$ の *lift* とする。(即ち、$\pi(\alpha) = \bar{\alpha}$)　$E : y^2 + xy = x^3 - \alpha^2$ とする。

Proposition 3.2.2 ([1] p.13)
$\exists a, b \in \mathbf{Z}_q, a \equiv 1 + 4\alpha + 8\alpha^2 \bmod 16, b \equiv 1 - 4\alpha + 8\alpha^2 \bmod 16$　*s.t.*　$E \cong E_{a,b}$
ここで、$E_{a,b} : y^2 = x(x - a^2)(x - b^2)$

$M(a,b) := (\frac{a+b}{2}, \sqrt{ab})$　$E_{M(a,b)} : y^2 = x(x - (\frac{a+b}{2})^2)(x - \sqrt{ab}^2)$ とする。

Proposition 3.2.3 ([1] p.15)
$\phi : E_{a,b} \to E_{M(a,b)}$　2-isogeny (次数が 2 の isogeny) で、$ker\phi = \{O, (0,0)\}$, $ker\hat{\phi} = \{O, ((\frac{a+b}{2})^2, 0)\}$, $\hat{\phi} * (\omega) = \omega$ となるものが存在する。
ここで、$ker\phi := \{P \in E_{a,b} | \phi(P) = O\}$、$\omega$ は *invariant differential* ([2] p.46)
$\hat{\phi} * \omega$ はその引き戻し ([2] p.35)

3.3 canonical lift

$E/\mathbf{Z}_q$ が $\bar{E}/\mathbf{F}_q$ の *lift* $\overset{def}{\iff} \pi(E) = \bar{E}$ (E の定義方程式の係数を π で移したものが $\bar{E}$ の定義方程式)

Theorem 3.3.1 (Lubin-Serre-Tate [1] p.17)
$\bar{E}$ を $\mathbf{F}_q$ 上の楕円曲線、$j(\bar{E}) \notin \mathbf{F}_4$ とする。

このとき次を満たす E の *lift* $\mathcal{E}/\mathbf{Z}_q$ が同型を除いて唯一つ存在する。

$$End(\mathcal{E}) \cong End(\bar{E}) \qquad (isogeny\text{の係数を}reduction\text{する写像で同型}) \tag{2}$$

$\mathcal{E}$ を $\bar{E}$ の *canonical lift* という。

Propsition 3.3.2
$\mathcal{E}, \mathcal{E}'$ をそれぞれ、E, E' の canonical lift とする。このとき次の同型が成立。

$$Hom(\mathcal{E}, \mathcal{E}') \cong Hom(E, E') \qquad (isogeny\text{の係数を}reduction\text{する写像で同型}) \tag{3}$$

3.4 $Tr(Fr_q)$ の計算

以上の準備の元、$Tr(Fr_q)$ を計算する。$\mathcal{E}$ を $\bar{E}$ の canonical lift とする。
$\widetilde{Fr_q} \in End(\mathcal{E})$ を Fr_q の lift とする。即ち、$End(\mathcal{E}) \cong End(\bar{E})$ において、Fr_q に対応する $End(\mathcal{E})$ の元とする。

Proposition 3.4.1
$Tr(\widetilde{Fr_q}) = Tr(Fr_q)$

proof
$t = Tr(Fr_q) \quad d = \deg Fr_q \quad \tilde{t} = Tr(\widetilde{Fr_q}) \quad \tilde{d} = \deg \widetilde{Fr_q}$ とする。
楕円曲線 E に対して、$End(E) \to End(T_l(E))$ は単射準同型であるから、
$Fr_q \circ Fr_q - [t] \circ Fr_q + [d] = [0] \qquad \widetilde{Fr_q} \circ \widetilde{Fr_q} - [\tilde{t}] \circ \widetilde{Fr_q} + [\tilde{d}] = [0]$
また、$End(\mathcal{E}) \cong End(\bar{E}) \quad \widetilde{Fr_q} \to Fr_q$ より
$Fr_q \circ Fr_q - [\tilde{t}] \circ Fr_q + [\tilde{d}] = [0] \qquad \widetilde{Fr_q} \circ \widetilde{Fr_q} - [t] \circ \widetilde{Fr_q} + [d] = [0]$
よって、$[\tilde{t} - t] \circ Fr_q = [\tilde{d} - d] \qquad [\tilde{t} - t] \circ \widetilde{Fr_q} = [\tilde{d} - d]$
両辺の次数を考えると、$(\tilde{t} - t)^2 d = (\tilde{d} - d)^2 \qquad (\tilde{t} - t)^2 \tilde{d} = (\tilde{d} - d)^2$
よって、$(\tilde{t} - t)^2 (\tilde{d} - d) = 0$
いずれの場合も $\tilde{t} = t$, $\tilde{d} = d$ となる。

Proposition 3.4.2
$(\widetilde{\widetilde{Fr_q}}) * \omega = \mu\omega$ とすると、$\mu \in \mathbf{Z}_q^\times$ であり、$Tr(Fr_q) = \mu + \frac{q}{\mu}$
proof
$t = Tr(Fr_q), \quad \widetilde{Fr_q} * \omega = \lambda\omega$ とする。
$\widetilde{Fr_q} \circ \widetilde{Fr_q} - [t] \circ \widetilde{Fr_q} + [q] = [0]$ より $\quad \lambda^2 - t\lambda + q = 0$
Newton 法より $x^2 - tx + q$ は $\mathbf{Z}_q$ に根を持つことがわかる。その根は λ, $\frac{q}{\lambda} \in \mathbf{Z}_q$ である。
よって、$t = \lambda + \frac{q}{\lambda}$
また、$\widetilde{Fr_q} \circ Fr_q = [q]$ より、$\lambda = \frac{q}{\mu} \quad t = \mu + \frac{q}{\mu}$
また、$\bar{\mu} \in \mathbf{F}_q$ (μ を reduction したもの) は $\widehat{Fr_q} * \bar{\omega} = \bar{\mu}\bar{\omega}$ を満たす。
$\widehat{Fr_q}$ は separable であるから、$\bar{\mu} \neq 0$ となる。よって、$\mu \in \mathbf{Z}_q^\times$

Proposition 3.4.3 ([1] p.17)
$\bar{E}$ の canonical lift $\mathcal{E}$ として次の形のものがとれる。

$$\mathcal{E}: \qquad y^2+xy=x^3-\alpha^2 \qquad \exists\alpha\in\mathbf{Z}_q \qquad \pi(\alpha)=\bar{\alpha} \tag{4}$$

Proposition 3.2.2 より、$\exists a\equiv 1+4\alpha+8\alpha^2 \bmod 16,\ \exists b\equiv 1-4\alpha+8\alpha^2 \quad s.t. \quad \mathcal{E}\cong\mathcal{E}_{a,b}$
ここで $\mathcal{E}_{a,b}: y^2=x(x-a^2)(x-b^2)$
$(a_1,b_1)=(\frac{a+b}{2},\sqrt{ab}) \qquad (a_n,b_n)=(\frac{a_{n-1}+b_{n-1}}{2},\sqrt{a_{n-1}b_{n-1}}) \quad (n\geq 2)$ と帰納的に定義する。
$\mathcal{E}_{a_n,b_n}: y^2=x(x-{a_n}^2)(x-{b_n}^2) \qquad \Sigma\mathcal{E}_{a_n,b_n}: y^2=x(x-\Sigma{a_n}^2)(x-\Sigma{b_n}^2)$ とする。
Σ は右の図式が可換となるような唯一つの $Gal(\mathbf{Q}_q/\mathbf{Q}_2)$ の元。

$$\begin{array}{ccc}\mathbf{Z}_q & \xrightarrow{\Sigma} & \mathbf{Z}_q\\ \downarrow & & \downarrow\\ \mathbf{F}_q & \xrightarrow{\sigma} & \mathbf{F}_q\end{array}$$

$\sigma: \mathbf{F}_q\longrightarrow\mathbf{F}_q \qquad x\longrightarrow x^2$

$\Sigma\mathcal{E}: y^2+xy=x^3-\Sigma\alpha^2$ は $\sigma\bar{E}: y^2+xy=x^3-\sigma\bar{\alpha}^2$ の canonical lift
$\Sigma\mathcal{E}\cong\Sigma\mathcal{E}_{a,b}$

Proposition 3.4.4 ([1] p.20)
$\widetilde{Fr_2}: \mathcal{E}_{a,b}\longrightarrow\Sigma\mathcal{E}_{a,b}$ を $Fr_2: \bar{E}\longrightarrow\sigma\bar{E} \quad (x,y)\longrightarrow(x^2,y^2)$ の lift とする。
$\phi: \mathcal{E}_{a,b}\longrightarrow\mathcal{E}_{a_1,b_1}$ を Proposition 3.2.3 におけるものとする。
このとき次の図式を可換にする同型 $\lambda: \mathcal{E}_{a_1,b_1}\longrightarrow\Sigma\mathcal{E}_{a,b}$ が存在する。

$$\begin{array}{ccc}& & \mathcal{E}_{a_1,b_1}\\ & \overset{\phi}{\nearrow} & \downarrow\lambda\\ \mathcal{E}_{a,b} & \xrightarrow{\widetilde{Fr_2}} & \Sigma\mathcal{E}_{a,b}\end{array}$$

この操作を繰り返すことにより、次の図式を得る。

$$\begin{array}{ccccccccccc}
 & & & & & & & & \mathcal{E}_{a_{N+1},b_{N+1}} & & \\
 & & & & & & & \overset{\phi_N}{\nearrow} & \downarrow\cong\lambda_N & & \\
 & & & & & & \mathcal{E}_{a_N,b_N} & \longrightarrow & \Sigma\mathcal{E}_{a_N,b_N} & & \\
 & & & & & \nearrow & \downarrow\cong & & \downarrow\cong & & \\
 & & & & \mathcal{E}_{a_{N-1},b_{N-1}} & \longrightarrow & \Sigma\mathcal{E}_{a_{N-1},b_{N-1}} & \longrightarrow & \Sigma^2\mathcal{E}_{a_{N-1},b_{N-1}} & & \\
 & & & \nearrow & & & \downarrow\cong & & \downarrow\cong & & \\
 & & & . & & & . & & . & & \\
 & & \overset{\phi_1}{\nearrow} & & & & \downarrow\cong & & \downarrow\cong\lambda_1 & & \\
 & & \mathcal{E}_{a_1,b_1} & \longrightarrow & . & . & . \longrightarrow & \Sigma^{N-1}\mathcal{E}_{a_1,b_1} & \longrightarrow & \mathcal{E}_{a_1,b_1} & \\
 & \nearrow & \downarrow\cong & & & & \downarrow\cong & & \downarrow\cong & & \\
\mathcal{E}_{a,b} & \xrightarrow{\widetilde{Fr_2}} & \Sigma\mathcal{E}_{a,b} & \longrightarrow & . & . & . \longrightarrow & \mathcal{E}_{a,b} & \longrightarrow & \Sigma\mathcal{E}_{a,b} & \\
\uparrow\cong & & \uparrow\cong & & & & & \uparrow\cong & & \uparrow\cong & \\
\mathcal{E} & \xrightarrow{\widetilde{Fr_2}} & \Sigma\mathcal{E} & \longrightarrow & . & . & . \longrightarrow & \mathcal{E} & \longrightarrow & \Sigma\mathcal{E} & \\
| & & | & & & & & | & & | & \\
\bar{E} & \xrightarrow{Fr_2} & \sigma\bar{E} & \longrightarrow & . & . & . \longrightarrow & \bar{E} & \longrightarrow & \sigma\bar{E} &
\end{array}$$

この図式より、次が成立する。

Proposition 3.4.5
$\phi:=\phi_N\circ\phi_{N-1}\circ\cdots\circ\phi_1 \qquad \lambda:=\lambda_1\circ\lambda_2\circ\cdots\circ\lambda_N$ とする。次が成立。

$$\widetilde{Fr_q} = \lambda \circ \phi \tag{5}$$

ここで、$\widetilde{Fr_q} : \mathcal{E}_{a_1,b_1} \to \mathcal{E}_{a_1,b_1}$ は $Fr_q : \sigma\bar{E} \to \sigma\bar{E}$ の lift

$\widehat{\widetilde{Fr_q}} = \widehat{\phi} \circ \widehat{\lambda}$ である。ここで、$\widehat{\phi} * \omega = \omega$ であったから、$(\widehat{\widetilde{Fr_q}}) * \omega = \widehat{\lambda} * \omega$
$\widehat{\lambda} = {\lambda_N}^{-1} \circ \cdots \circ {\lambda_1}^{-1}$

$$\begin{array}{ccc} & & \Sigma^{N-k}\mathcal{E}_{a_{k+1},b_{k+1}} \\ & \phi_k^{(N-k)} \swarrow & \downarrow \cong \lambda_k \\ \Sigma^{N-k}\mathcal{E}_{a_k,b_k} & \xleftarrow{\widehat{\widetilde{Fr_2}}} & \Sigma^{N-k+1}\mathcal{E}_{a_k,b_k} \end{array}$$

$ker(\widehat{\widetilde{Fr_2}}) = \{\mathcal{O}, (\Sigma^{N-k+1}{a_k}^2, 0)\}$ ([1] p. 21)
$ker(\phi_k^{(N-k)}) = \{\mathcal{O}, (\Sigma^{N-k}{a_{k+1}}^2, 0)\}$
$\lambda_k : (x, y) \to (u^2x, u^3y) \qquad u = \pm\frac{\Sigma^{N-k+1}a_k}{\Sigma^{N-k}a_{k+1}}$
$({\lambda_k}^{-1}) * \omega = \mu_k\omega$ とすると、$\mu_k = \pm\frac{\Sigma^{N-k+1}a_k}{\Sigma^{N-k}a_{k+1}}$
$\widehat{\lambda} * \omega = \mu\omega$ とすると、$\mu = \prod_{k=1}^{N}\mu_k = \pm\frac{a_1}{a_{N+1}}$ よって、$Tr(Fr_q) = \pm(\frac{a_1}{a_{N+1}} + q\frac{a_{N+1}}{a_1})$

$m = [\frac{N}{2} + 2]$ とする。この議論を $\sigma^{m-3}\bar{E}$ から始めることで、同様にして、$Tr(Fr_q) = \pm(\frac{a_{m-3}}{a_{m+N-3}} + q\frac{a_{m+N-3}}{a_{m-3}})$
$Tr(Fr_q) \equiv \pm\frac{a_{m-3}}{a_{m+N-3}} \mod 2^m$
a_{m-3}, a_{m+N-3} は $\bar{E}$ の canonical lift から求まるものなので、直接計算するのは難しい。しかし、次のようにして、$\bar{E}$ の勝手な lift から、近似的に計算できる。
$\alpha' \in \mathbf{Z}_q$ を $\bar{\alpha}$ の勝手な lift とする。$a'_0 = 1 + 4\alpha' \mod 16, \quad b'_0 = 1 - 4\alpha' \mod 16$
$a'_n = \frac{a'_{n-1}+b'_{n-1}}{2} \mod 2^{n+4}, \quad b'_n = \sqrt{a'_{n-1}b'_{n-1}} \mod 2^{n+4}$ と定義する。
このとき、$\frac{a_n}{a_{n+1}} \equiv \frac{a'_n}{a'_{n+1}} \mod 2^{n+3}$ が成立する。([1] p.24)
よって、$\frac{a_{m-3}}{a_{m+N-3}} \equiv \frac{a'_{m-3}}{a'_{m+N-3}} \mod 2^m$

$$Tr(Fr_q) \equiv \pm\frac{a'_{m-3}}{a'_{m+N-3}} \mod 2^m \tag{6}$$

そして、Theorem 3.1(2) より、$Tr(Fr_q)$ が完全に求まる。

4 テータ関数を用いる方法

テータ関数を用いた方法を紹介する。これは、Mestre の方法を一般の曲線に拡張する際に必要となる。
$\bar{E} : y^2 + xy = x^3 - \bar{\alpha}^2$, $\alpha \in \mathbf{Z}_q$ を $\bar{\alpha} \in \mathbf{F}_q$ の lift, $E : y^2 + xy = x^3 - \alpha^2$ とする。

$f(X) \in \mathbf{Z}[X]$ を $\mathbf{F}_q$ の定義式、即ち $\mathbf{F}_q = \mathbf{F}_2[X]/ < f(X) >$ とする。
$\mathbf{C}$ の部分体として $K = \mathbf{Q}[X]/ < f(X) >$ とすると、K は $\mathbf{Q}$ の N 次拡大である。
$\mathbf{Q}_q = \mathbf{Q}_2[X]/ < f(X) >$ であり、$\mathbf{Q}$ は $\mathbf{Q}_q$ の中で稠密であるから、K は $\mathbf{Q}_q$ の中で稠密な部分体と思える。
つまり、$\mathbf{Q}_q$ の元を $\mathbf{C}$ の元で近似できる。

$a', b' \in K$ を $a' \equiv 1 + 4\alpha \mod 16$, $b' \equiv 1 - 4\alpha \mod 16$ となるようにとれる。

$E_{a',b'}/\mathbf{C} : y^2 = x(x-a'^2)(x-b'^2)$ とする。
$E_{a',b'}$ の周期行列を τ_0 とする。$\tau_0 \in \mathbf{C}$, $Im(\tau_0) > 0$
$z, \tau \in \mathbf{C}$, $Im(\tau) > 0$ に対して、$\theta(z,\tau) := \sum_{n=-\infty}^{\infty} exp(\pi i n^2 \tau + 2\pi i n z)$ とする。$\theta(z,\tau)$ をテータ関数という。

Proposition 4.1 ([4])

$$Tr(Fr_q) \equiv \pm \frac{\theta(0, 2^{m-1}\tau_0)^2}{\theta(0, 2^{m+N-1}\tau_0)^2} \mod 2^m \qquad m = [\tfrac{N}{2} + 2] \tag{7}$$

Theorem 4.2 (Riemann の 2 倍公式 [4])

$$\theta(0, 2\tau)^2 = \tfrac{1}{2}\{\theta(0,\tau)^2 + \theta(\tfrac{1}{2},\tau)^2\} \tag{8}$$

$$\theta(\tfrac{1}{2}, 2\tau)^2 = \theta(0,\tau)\theta(\tfrac{1}{2},\tau) \tag{9}$$

よって、$\theta(0, 2^{m-1}\tau_0)^2$, $\theta(0, 2^{m+N-1}\tau_0)^2$ は $\theta(0,\tau_0)^2$, $\theta(\frac{1}{2},\tau_0)^2$ から計算できる。
つまり、$\theta(0,\tau_0)^2$, $\theta(\frac{1}{2},\tau_0)^2$ を $E_{a',b'}$ の定義方程式から求められるかが問題となる。
それに答えるのが次の定理である。

Theorem 4.3 (Thomae-Fay [5])
$\mathbf{C}$ 上の楕円曲線 $E : y^2 = x(x-a)(x-b)$ に対して、その周期行列を τ とする。
このとき、$\exists \zeta \in \mathbf{C} \quad s.t. \quad \theta(0,\tau)^4 = \zeta a, \quad \theta(\frac{1}{2},\tau)^4 = \zeta b$

これより、$Tr(Fr_q) \equiv \pm \frac{a'_{m-1}}{a'_{m+N-1}} \mod 2^m$ が示せる。
ここで $(a'_1, b'_1) = (\frac{a'+b'}{2}, \sqrt{a'b'})$, $(a'_n, b'_n) = (\frac{a'_{n-1}+b'_{n-1}}{2}, \sqrt{a'_{n-1}b'_{n-1}})$ と帰納的に定義した。

5 高い種数の曲線への一般化

C を $\mathbf{F}_q$ 上定義された、種数 g の非特異な射影曲線とする。C の Jacobi 多様体を $Pic^0(C)$ とする。([2])
$Pic^0_{\mathbf{F}_q}(C) := \{D \in Pic^0(C) \mid \sigma D = D \quad for\ \forall \sigma \in Gal(\overline{\mathbf{F}_q}/\mathbf{F}_q)\}$ とし、$Pic^0(C)$ の $\mathbf{F}_q$ 有理点という。
$Pic^0_{\mathbf{F}_q}(C)$ は $Pic^0(C)$ の有限部分群になる。$\sharp Pic^0_{\mathbf{F}_q}(C)$ を求めることを考える。

$F : C \longrightarrow C \qquad [x_0 : \cdots : x_n] \longrightarrow [x_0{}^q : \cdots : x_n{}^q] \quad (q = 2^N)$ とする。(q 乗 Frobenius 写像)
l を奇素数とする。$J[l] := \{D \in Pic^0(C) \mid l \cdot D = 0\}$ とする。$J[l] \cong (\mathbf{Z}/l\mathbf{Z})^{2g}$ となる。
$[l] : J[l^{n+1}] \longrightarrow J[l^n] \qquad D \longrightarrow l \cdot D$ とすると、$\{J[l^n], [l]\}_{n \geq 1}$ は射影系をなす。
$T_l := \lim_{\leftarrow n} J[l^n]$ (逆極限) として、$Pic^0(C)$ の l 進 Tate 加群という。
T_l は rank が $2g$ の自由 $\mathbf{Z}_l$ 加群になる。
F により、$\mathbf{Z}_l$ 準同型 $\tilde{F} : T_l \to T_l$ が自然に誘導される。
$\tilde{F}$ の固有多項式を χ_F とすると、χ_F は 2^g 次の $\mathbf{Z}$ 係数 monic 多項式となる。(χ_F は l によらない)
$\chi_F(x) = (x-\pi_1)\cdots(x-\pi_g)(x-\bar{\pi_1})\cdots(x-\bar{\pi_g}) \quad \bar{\pi_i} = \frac{q}{\pi_i}$ と分解できる。

多変数のテータ関数を次のように定義する。
$z \in \mathbf{C}^g$, $\Omega \in \mathcal{H}_g := \{\Omega \in M_g(\mathbf{C}) \mid \Omega^T = \Omega,\ Im(\Omega) > 0\}$ に対して、
$\theta(z,\Omega) := \sum_{N \in \mathbf{Z}^g} exp(\pi i N^T \Omega N + 2\pi i N^T z)$

Theorem 5.1 (Hasse-Weil)
$\sharp Pic^0_{\mathbf{F}_q}(C) = \chi_F(1)$

以後 C を超楕円曲線とする。
$\pi_1 \cdots \pi_g$ (積) が求まれば、$\chi_F(x)$ を決定することが出来る。([6])
C に対して、K 上の曲線 X をうまく選ぶことができて、X の周期行列を $\Omega_0 \in \mathcal{H}_g$ とすると
$\pi_1 \cdots \pi_g \equiv \pm \dfrac{\theta(0, 2^{m-1}\Omega_0)^2}{\theta(0, 2^{m+N-1}\Omega_0)^2} \mod 2^m$ となる。([4])

Theorem 5.2 (Riemann の 2 倍公式 [4])
$\epsilon \in (\frac{1}{2}\mathbf{Z}/\mathbf{Z})^g$に対して、 $\theta(\epsilon, 2\Omega)^2 = \frac{1}{2^g} \sum_{e \in (\frac{1}{2}\mathbf{Z}/\mathbf{Z})^g} \theta(\epsilon + e, \Omega)\, \theta(e, \Omega)$

よって、$\theta(0, 2^{m-1}\Omega_0)^2$, $\theta(0, 2^{m+N-1}\Omega_0)^2$ は $\{\theta(\epsilon, \Omega_0)\}_{\epsilon \in (\frac{1}{2}\mathbf{Z}/\mathbf{Z})^g}$ から求まる。
よって、$\{\theta(\epsilon, \Omega_0)\}_{\epsilon \in (\frac{1}{2}\mathbf{Z}/\mathbf{Z})^g}$ を X の定義方程式から求められればよい。

Theorem 5.3 (Thomae-Fay [4],[5])
X を $y^2 = (x - a_1) \cdots (x - a_{2g+2})$ で定義される、$\mathbf{C}$ 上の超楕円曲線とする。
$S = \{a_1, a_3, \cdots, a_{2g+1}\}$ $U_i = \{a_{2i-1}, a_{2i}\}$ $i = 1, \cdots, g$ $\epsilon = (\epsilon_1, \cdots, \epsilon_g)$ $\epsilon_i \in \frac{1}{2}\mathbf{Z}/\mathbf{Z}$
$U_\epsilon = \cup_j U_j$ (j は $\epsilon_j \notin \mathbf{Z}$ となる j をわたる。) $S \circ U_\epsilon := S \cup U_\epsilon - S \cap U_\epsilon$ とする。x_{a_i} を a_i の x 座標とする。
X の周期行列を Ω とする。このとき、ϵ に依らない $\zeta \in \mathbf{C}$ が存在して、次が成立する。

$$\theta(\epsilon, \Omega)^4 = \pm\zeta \prod_{a_i, a_j \in S \circ U_\epsilon \; i<j} (x_{a_i} - x_{a_j}) \prod_{a_i, a_j \notin S \circ U_\epsilon \; i<j} (x_{a_i} - x_{a_j}) \tag{10}$$

これにより、$\sharp Pic^0_{\mathbf{F}_q}(C)$ を求めることができる。
この方法を超楕円を越える曲線に一般化するには Thomae-Fay の公式をその曲線まで拡張することが必要である。
しかし現在、この公式は一般の非特異射影曲線にまで拡張されていない。よって Thomae-Fay の公式をより広い代数曲線まで拡張することが今後の課題となる。一般化する代数曲線は具体的には 6 で述べる三浦曲線を考えている。
(現在のところ、$(a, b) = 1$, $y^a = f(x)$, $\deg f(x) = b$ の形の曲線 (後に述べる三浦曲線に含まれる) にまでは拡張されている。(Bershadsky-Radul, 1986))

6 三浦曲線

この章では、三浦晋示氏により提案された代数曲線のクラスである、三浦曲線の定義を述べる。([7])
ここでは、$\mathbf{N}$ は 0 以上の整数全体を表すものとする。
$a_1, \cdots, a_t \in \mathbf{N}\backslash\{0\}$, $A_t = (a_1, \cdots, a_t)$, $\{a_1, \cdots, a_t\}$ の最大公約数は 1, $< A_t >= a_1\mathbf{N} + \cdots + a_t\mathbf{N}$ とする。
$\Psi : \mathbf{N}^t \to < A_t >$ $(n_1, \cdots, n_t) \to \sum_{i=1}^t a_i n_i$ とする。
$\mathbf{N}^t$ の順序 $\succ$ を次で定義する。
$M = (m_1, \cdots, m_t)$ $N = (n_1, \cdots, n_t) \in \mathbf{N}^t$ に対して、
$M \succ N \overset{\text{def}}{\iff} \Psi(M) > \Psi(N)$ 又は、$\Psi(M) = \Psi(N)$ のときは $m_1 = n_1$, $\cdots$, $m_{i-1} = n_{i-1}$, $m_i \leq n_i$
$\succ$ は整列順序になる。

$B(A_t) \subseteq \mathbf{N}^t$ を $B(A_t) := \{M(a) \mid a \in < A_t >\}$
ここで、$M(a) \in \mathbf{N}^t$ とは $\Psi(M) = a$ を満たす $M \in \mathbf{N}^t$ の中で $\succ$ の意味で最小の元とする。
$V(A_t) := \{L \in \mathbf{N}^t \backslash B(A_t) \mid L = M + N,\ M \in \mathbf{N}^t \backslash B(A_t),\ N \in \mathbf{N}^t \Rightarrow N = (0, \cdots, 0)\}$ とする。
$V(A_t)$ は有限集合で、$2 \leq i \leq t$ について $\{0\}^{i-1} \times \mathbf{N} \times \{0\}^{t-i} \cap V(A_t)$ は唯一つの元からなる。これを N_i とする。
$SV(A_t) := \{N_i \mid 2 \leq i \leq t\}$ とする。

以上の準備の下、三浦曲線を定義する。
F を完全体 $a_1, \cdots, a_t \in \mathbf{N} \backslash \{0\}$, $A_t = (a_1, \cdots, a_t)$, $\{a_1, \cdots, a_t\}$ の最大公約数は 1 とする。
$\{F_M \mid M \in V(A_t)\} \subseteq F[X_1, \cdots, X_t]$ を次の条件 $(D\,1), (D\,2)$ を満たすようにとる。

$(D\,1)$ $F_M = X^M + \alpha_L X^L + \sum_N \alpha_N X^N$
ここで、$X^M = {X_1}^{m_1} \cdots {X_t}^{m_t}$ $M = (m_1, \cdots, m_t)$, $\alpha_L, \alpha_N \in F$, $\alpha_L \neq 0$
L は $\Psi(M) = \Psi(L)$ となる $B(A_t)$ の元、$\sum_N$ の N は $\{N \in B(A_t) \mid \Psi(N) < \Psi(M)\}$ をわたる。

$(D\,2)$ $Span_F\{X^N \mid N \in B(A_t)\} \cap (\{F_M \mid M \in V(A_t)\}) = \{0\}$
ここで、$Span_F\{X^N \mid N \in B(A_t)\}$ は $\{X^N \mid N \in B(A_t)\}$ で生成される F 上のベクトル空間、
$(\{F_M \mid M \in V(A_t)\})$ は $\{F_M \mid M \in V(A_t)\}$ で生成される、$F[X_1, \cdots, X_t]$ のイデアルである。

$I := (\{F_M \mid M \in V(A_t)\})$, $R := F[X_1, \cdots, X_t]/I$ とする。

Proposition 6.1
(1) I は素イデアル
(2) R の商体を K とすると、K の F 上の超越次数は 1

よって、I により、$\bar{F}^t$ のアフィン代数曲線が定義される。これを三浦曲線という。
実際に三浦曲線を構成する際、$(D\,1)$ を満たすようにとるのは簡単だが、それが $(D\,2)$ を満たすかどうかを判定するのは難しい。
つまり次の命題は有用である。

Proposition 6.2
$SV(A_t) = V(A_t)$ ならば、$(D\,1)$ を満たすように $\{F_M \mid M \in V(A_t)\}$ をとれば、
$(D\,2)$ は自動的に満たされる。

三浦曲線の例
(1) $t = 2$, $a_1 = 2$, $a_2 = 3$ のとき
$F(x, y) = y^2 + (\alpha_1 x + \alpha_0)y + \beta_3 x^3 + \beta_2 x^2 + \beta_1 x + \beta_0 = 0$ $(\alpha_i, \beta_i \in F)$ で定義される曲線（楕円曲線）
(2) $t = 2$, $a_1 = 2$, $a_2 = 2g + 1$ のとき
$F(x, y) = y^2 + (\alpha_g x^g + \cdots + \alpha_1 x + \alpha_0)y + \beta_{2g+1} x^{2g+1} + \cdots + \beta_1 x + \beta_0 = 0$ $(\alpha_i, \beta_i \in F)$ で定義される曲線（超楕円曲線）
(3) $t = 2$, $a_1 = a$, $a_2 = b$, $(a, b) = 1$ のとき
$F(x, y) = \sum_{0 \leq i \leq b,\ 0 \leq j \leq a,\ 0 \leq ai + bj \leq ab} \alpha_{i,j} x^i y^j = 0$, $\alpha_{i,j} \in F$, $\alpha_{0,a} \neq 0$ で定義される曲線（$C_{a,b}$ 曲線）

つまり、三浦曲線は楕円曲線、超楕円曲線を含む代数曲線のクラスである。

7 今後の課題

代数曲線暗号の安全性を確かめる上で代数曲線の Jacobi 多様体の有理点の個数を求めることはとても大切であり、楕円曲線の場合に最も効率のよい Mestre の方法を一般の代数曲線にも適用したい。その代数曲線としては三浦曲線を使う。しかしそれには曲線の定義方程式から、それに対応するテータ定数を求める Thomae-Fay の公式を三浦曲線に一般化することが必要不可欠である。それがまず第一の課題であり、その後、一般化された Thomae-Fay の公式を使って、三浦曲線の Jacobi 多様体の有理点の個数を実際に計算機を用いて計算し、計算量、計算時間を評価したい。

参 考 文 献

[1] Marc Skov Madsen, The AGM-method of Point Counting on Ordinary Elliptic Curves over Finite Fields of Characteristic 2, 2002, http://home.imf.au.dk/marc/doc/phd/progress/agm.pdf

[2] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics 106, Springer, 1985

[3] A. Enge, Elliptic curves and their applications to cryptography, Kluwer Academic Publishers, 1999

[4] Reynald Lercier, David Lubicz, A Quasi Quadratic Time Algorithm for Hyperelliptic Curve Point Counting, The Ramanujan Journal 12, 2006, 399–423

[5] D. Mumford, Tata Lectures on Theta 2, Birkhauser, 1984

[6] J.F. Mestre, Algorithmes pour compter des points en petite caracteristique en genre 1 et 2, http://people.math.jussieu.fr/~mestre/rennescrypto.ps

[7] S. Miura, Algebraic geometric codes on certain plane curves (Japanese), IEICE Trans. Fundamentals J75-A, 1992, 1735–1745

[8] D. Mumford, Tata Lectures on Theta 1, Birkhauser, 1983

[9] Takakazu Satoh, The Canonical Lift of an Ordinary Elliptic Curve over a Finite Field and its Point Counting, J. Ramanujan Math. Soc. 15, 2000, 247–270

[10] J. Lubin, J.-P. Serre, J. Tate, Elliptic Curves and Formal Groups, 1964, http://www.ma.utexas.edu/users/voloch/lst.html

[11] Fre Vercauteren, Canonical Lift Methods, 2005, http://homes.esat.kuleuven.be/~fvercaut/talks/Satoh.pdf

[12] Berit Skjernaa, Satoh's algorithm in characteristic 2, Math. Comp. 72, 2003, 477–487

[13] 足立恒雄, 三宅克哉, 類体論講義, 日本評論社, 1998